Patent Application

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	MESSERGES ET AL.	EXAMINER:	ABYANEH
SERIAL NO.:	10/028,164	GROUP:	2133
FILED:	25 OCT 2001	CASE NO.:	CR00287M
TITLED:	A METHOD FOR EFFICIENT HASHING OF DIGITAL CONTENT		

Motorola, Inc.
Corporate Offices
1303 E. Algonquin Road
Schaumburg, IL 60196
May 31, 2005

Declaration Under 37 CFR §1.131

Each of the undersigned, Thomas Messerges, Ezzat Dabbish, Larry Puhl, and Douglas Kuhlman declare the following:

1. Prior to March 21, 2001, we conceived of the invention in the United States now claimed in US Patent application number 10/028,164.

2. As evidence of the conception date of the pending application, enclosed is supporting materials in the form of true copies of original exhibits. These original exhibits were created by us in the United States and witnessed by a third party prior to March 21, 2001.

3. We exercised due diligence from prior to March 21, 2001 to October 25, 2001 to prepare and file the pending patent application number 10/028,164. During this time period, we continually worked toward preparing the pending patent application for filing with the USPTO.

4. All of the above statements made of our own knowledge are true and all statements made on information and belief are believed to be true.

5. We understand that willful false statements and the like are punishable by fine or imprisonment, or both (18 USC §1001) and may jeopardize the validity of the pending application or any patent issuing thereon.

Thomas Messerges — Date: 5-31-05

Ezzat Dabbish — Date: 5-31-05

Larry Puhl — Date: 5-31-2005

Douglas Kuhlman — Date: 5-31-2005

MOTOROLA LABS

Motorola Patent Committee

Disclosure Number	Date
CR00287M	February 15, 2004
Division(s): Corporate	
Patent Committee Action:	

Disclosure for Patent Committee Review
Submitted Pursuant to Employee Agreement
DISCLOSURE TYPE:

SHORT FORM [ ] When using the short form (single page), the review committee may request additional information before reaching a decision.

EXPANDED [X] Use additional pages in the expanded form if you feel more information will be necessary for the committee to reach a decision.

1. Title of Invention: A Method for Securely Binding Usage Rules to Digital Content

1a. Key Words: Digital Rights Management (DRM), Digital Content Content Protection, Hash, Certificate

2. Primary or contact point inventor(s) (Use your full first, middle and last names. Use page 2 of the expanded disclosure form for contributing inventors).

	Name	Signature	Dept. No.	Location/Rm. #	Phone Number
1)	Thomas S. Messerges		AE575	IL02 Rm 2712	847-576-5827
	Citizenship: US	SSN: 328-60-0086	Street: 151 Brookston Drive	City: Schaumburg	State: IL ZIP: 6019
2)	Ezzat A. Dabbish		AE575	IL02 Rm 2712	847-576-5377
	Citizenship: US	SSN: 329-50-0221	Street: 445 Adare Drive	City: Cary	State: IL ZIP: 6001
3)	Larry Puhl		AE579	IL02 Rm 2256	847-576-5463
	Citizenship: US	SSN: 338-38-6126	Street: 1231 Fawn Hallow	City: West Dundee	State: IL ZIP: 6011
4)	Douglas A. Kuhlman		AE575	IL02 Rm 2712	847-576-9675
	Citizenship: US	SSN: 510-88-0815	Street: 1447 Ashwood Ct	City: Elgin	State: IL ZIP: 6012

3. What was the problem(s) to be solved by the invention or what was the need(s) for the invention:

The popularity of digital content, such as MP3 music files, electronic games, and DVD movies, is growing at a tremendous rate. Portable, wireless devices are on the verge of making access to this digital content easier than ever. Content owners, however, are worried, that with the advent of these new devices, their digital content will become more susceptible to illicit copying and distribution. In order to avoid widespread piracy, like that prevalent on the Internet (e.g., Napster), there is a need for secure methods to distribute electronic content that are not subject to abuse.

Digital Rights Management (DRM) is a popular phrase used to describe the protection of rights and the management of rules related to accessing and processing digital information. These rights and rules govern various aspects of a digital object, such as who owns the object, how and when an object can be accessed, and how much an object may cost. Content owners hope to use a secure, tamper-resistant DRM system to enforce the rules associated with a digital object. If the rules say that a digital song cannot be copied, then the DRM system will not copy it. Likewise, if the rules say that playing a DVD movie will cost $3, then the DRM system will debit the consumer's credit card by $3. Hackers should not be able to overcome the enforcement of these rules or alter the content associated with these rules. In particular, hackers should not be able to alter digital objects or their rules without detection.

The problem of protecting digital objects and their rules is not straightforward. Hackers will likely have direct access to the digital objects and the rules. For example, objects and rules may be stored on the disk drive of a PC where they can be readily accessed by an editing program. Therefore, since hackers will be able to easily change bits in the digital objects or the rules, the DRM system will need to detect such changes.

The size of the digital object can become very large. For example, compressed digital songs are typically 3 to 5 Mbits and DVD movies can be orders of magnitude larger. Verifying that such a large digital object has not been altered can be very time consuming. Our invention solves this problem by providing an efficient method to detect changes in digital objects and their associated usage rules.

4. What is the prior art, and why doesn't it resolve the problem(s) or fulfill the need(s):

In our situation, the content and usage rules constitute a digital object that we refer to as a "content package". A well-known prior-ar method for authenticating the integrity of a digital object uses a digital signature scheme to sign a cryptographic hash of the object. A prio art solution using a digital signature scheme and hash to protect digital content is depicted in Figure 1. According to Figure 1, the first step is to encrypt the content. The content is encrypted with a secret key to protect it from being used by anyone other than content purchaser. The encrypted content is then cryptographically hashed to produce Hash(*EC*). This hash value is placed into the certificate *CCert*. The *CCer* certificate also contains the content's usage rules along with the content decryption key that is assigned to the content purchaser using public-key cryptography. Finally, a trusted authority digitally signs the certificate.

Verifying the authenticity of a content package is simple. The first step is to verify the signature of the digital signature of *CCert*. Once this signature is verified, the hash of the encrypted content is recalculated and compared to the value in the certificate. If digital signature is valid and the hash values match, then the content package is deemed authentic. The rendering of content can begin only after the content package has been authenticated.

The main problem with this prior-art solution is that it can take too long to calculate the hash of the entire content package. A user of a content rendering device expects rendering to begin immediately. After pressing the play button of an MP3 player, the song should start playing with minimal delay. If the prior-art method is used, then the hash of the entire content needs to be calculated before the usage rules can be verified. This could be very time consuming. For example, the estimated time to compute the SHA1 hash of a typical MP3 song, when using a 16 MHz MCore processor, is around 15 to 20 seconds. Clearly this is too long and a more efficient method is needed. More background on prior-art data authentication solutions can be found in standard cryptography textbooks such as:

Douglas R. Stinson, "Cryptography: Theory and Practice," CRC Press, 1995.

5. What is the invention being disclosed:

Our invention eliminates the need to calculate the hash of the entire content package before rendering the content. Instead, the hash is calculated incrementally and verified as the content is being rendered.

Our invention is depicted in Figure 2. As in the prior-art solution the first step is to encrypt the content. Next, however, the content is split into smaller "chunks". The cryptographic hash of each of these chunks is then calculated and stored into a "hash table". The entries of the hash table are then hashed to create an "overall hash". The overall hash is placed into the certificate *CCert* that is then signed by a trusted authority.

The advantages of our scheme become apparent when authenticating the content package. Figure 3 shows that our authentication procedure begins with a verification of the hash table. The overall hash of the hash table is recalculated and then compared to the hash value in the *CCert* certificate. If the hash values agree and the signature on *CCert* is valid, then the hash table and its binding to the usage rules is verified. Since the overall hash is not over the entire content, but just the hash table, it can be quickly calculated.

Once the overall hash has been authenticated, the hash of the individual chunks can be verified. Figure 4 shows our procedure for verifying the authenticity of a chunk. The first step is to recalculate the hash table entry of the chunk and compare it to the actual hash value in the hash table. Since the hash table has already been authenticated, agreement of the hash values implies that the chunk is authentic. It should be noted that the computation of a chunk's hash is not as time consuming as computing the hash of the entire content package. Also, this hash value can be calculated in parallel to the chunk decryption. Thus, rendering can begin almost immediately.

6. How does this invention resolve the problem(s) and fulfill the need(s) in a new way:
(Attach any drawings or diagrams you feel are necessary for clarification)

The problem of authenticating digital content and its binding to usage rules was solved using a divide-and-conquer approach. Our invention calls for the authentication to be conducted in two phases. The first phase provides assurance that the hash table is authentic and bound to the certificate and rules. This phase can be calculated very quickly since only the hash of the hash table needs to be computed. By hashing the hash table, hackers are prevented from deleting, adding, or rearranging the content chunks.

The second phase of our invention verifies the authenticity of every content bit. The hash of the content chunk is compared to the hash table entry to provide final assurance that the content is bound to the certificate and rules. This hash can be calculated one chunk at a time, parallel to decryption, to enable immediate rendering.

Our invention is even applicable to protecting extremely large content files (i.e., video). In this situation, the hash table can be very large and even calculating the overall hash becomes too slow. Our invention, with a minor modification, can handle this problem by allowing the hash table to be subdivided into chunks that are subsequently hashed and added to a secondary hash table. The resulting scheme then uses multiple layers of hash tables and a single certificate to authenticate all of the hash tables and the content.

Overall, the disclosed invention provides an efficient means to authenticate digital content and bind the content to usage rules. The security of our scheme is equivalent to prior art methods, while the efficiency is improved.

7. Date of conception: January, 2001 and if applicable, date first built (or written) and successfully tested:

8. **Product(s) this invention may be used in:**
Future Motorola pagers, mobile phones, automotive entertainment systems, and set-top boxes that handle digital content such as music books, and video.

9. **Date the first offer for sale was made for a product incorporating this invention:**
None, but there are plans to discuss our secure content distribution system with Vivendi/Universal and Disney.

10. **Date the first disclosure of this invention was made outside Motorola without a nondisclosure agreement:**
None, but disclosure during an SDMI meeting is being considered.

11. **Approvals:** 1) Technical Staff or Patent Liaison 2) Management (both required) – *Signing this form attests to the fact that you understand the inventio*

	Name/Signature		Dept. No.	Location/Rm. #	Phone Number
	Larry Pubi	Larry Pubi	AE579	IL02	6-5463
2)	STEVE LEVINE	Steve Levine	AE570	IL02	6-2107

12. **Witnesses:**
Witness: [signature] Date: 2/19/2001 Witness: [signature] Date: 2/19/01

13. **Contributing Inventor(s):** *Patent Department will determine legal inventorship*

5)

Name	Signature	Dept. No.	Location/Rm. #	Phone Number
Citizenship	**SSN**	**Street**	**City**	**State** / **ZIP**

6)

Name	Signature	Dept. No.	Location/Rm. #	Phone Number
Citizenship	**SSN**	**Street**	**City**	**State** / **ZIP**

7)

Name	Signature	Dept. No.	Location/Rm. #	Phone Number
Citizenship	**SSN**	**Street**	**City**	**State** / **ZIP**

8)

Name	Signature	Dept. No.	Location/Rm. #	Phone Number
Citizenship	**SSN**	**Street**	**City**	**State** / **ZIP**

14. **What is the business impact of having a patent on this invention, for Motorola and/or competition:**
It is in Motorola's interest to ensure that their products uphold the emerging security requirements for managing digital data, while also providing for an enjoyable user experience for our consumers. Our disclosed invention provides a novel method to improve a user's experience by ensuring that their content can be rendered without delays or interruptions due to annoying DRM requirements.

Being first to market with a Digital Rights Management system that does not hinder the end user will secure Motorola's leadership in the industry. Other organizations may mandate the use of our solution, in which case financial gains can be made from licensing and royalty fees. In addition orders for our products can be expected to increase as a result of our name being tied to a secure and user friendly solution.

15. **Expanded description; list any additional details you feel would be helpful in describing the invention:**

16. **Additional details concerning the prior art related to this invention:**

Attach any backup documents or provide any other information you feel would be helpful in determining the desirability of obtaining a patent on this invention. Any attachments that are critical to the disclosure of the invention should be witnessed.

See attached Figures 1 to 4.

Additional Information:

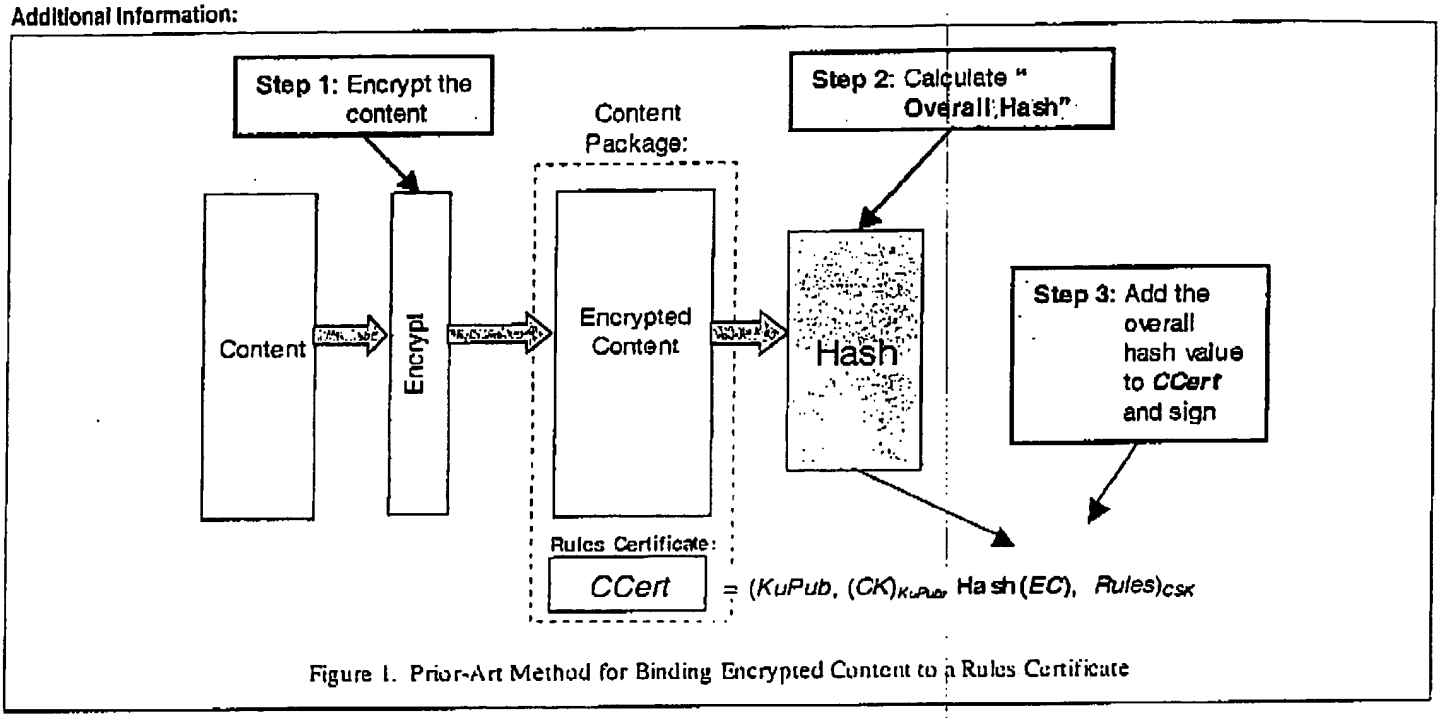

Figure 1. Prior-Art Method for Binding Encrypted Content to a Rules Certificate

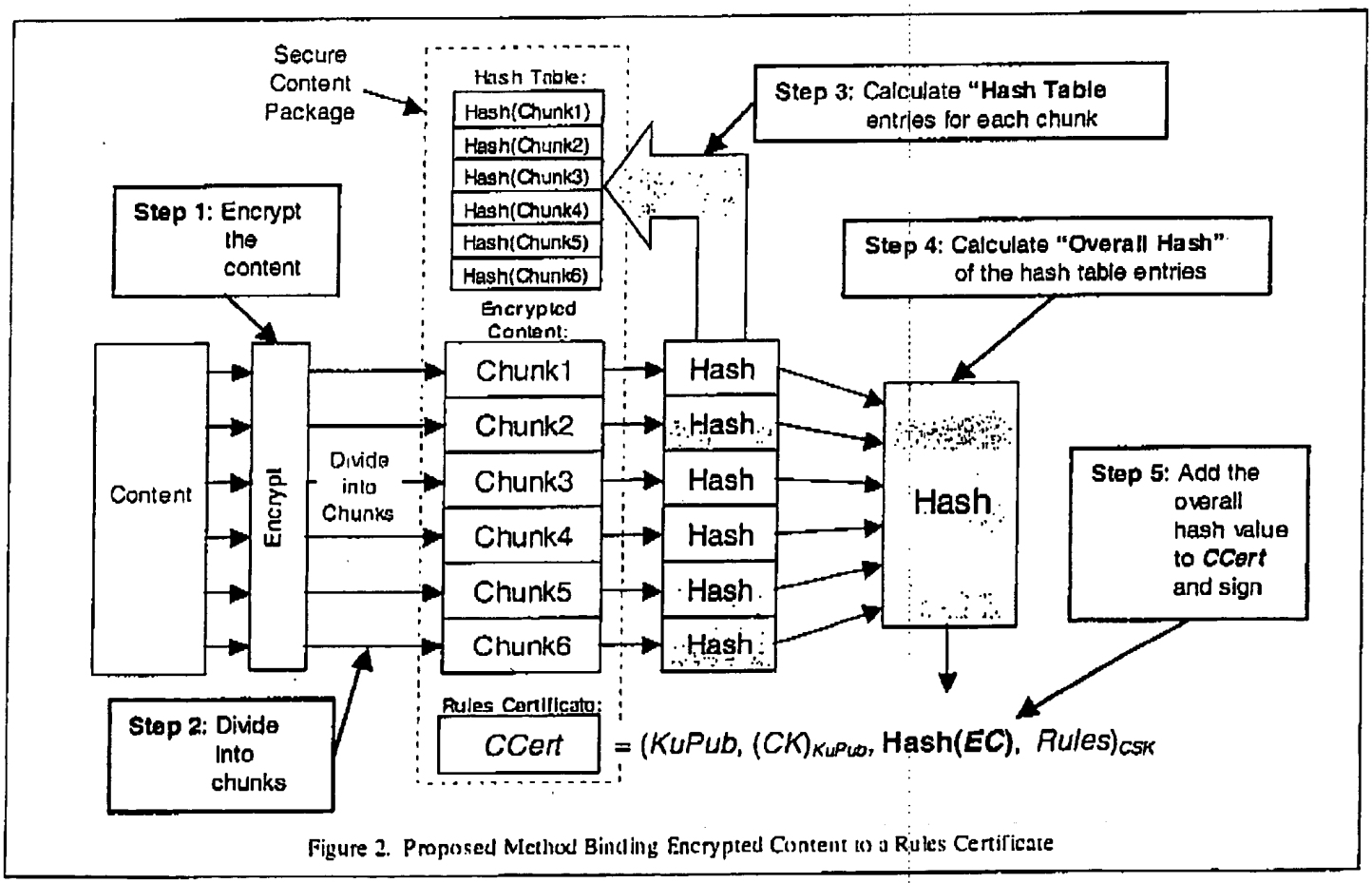

Figure 2. Proposed Method Binding Encrypted Content to a Rules Certificate

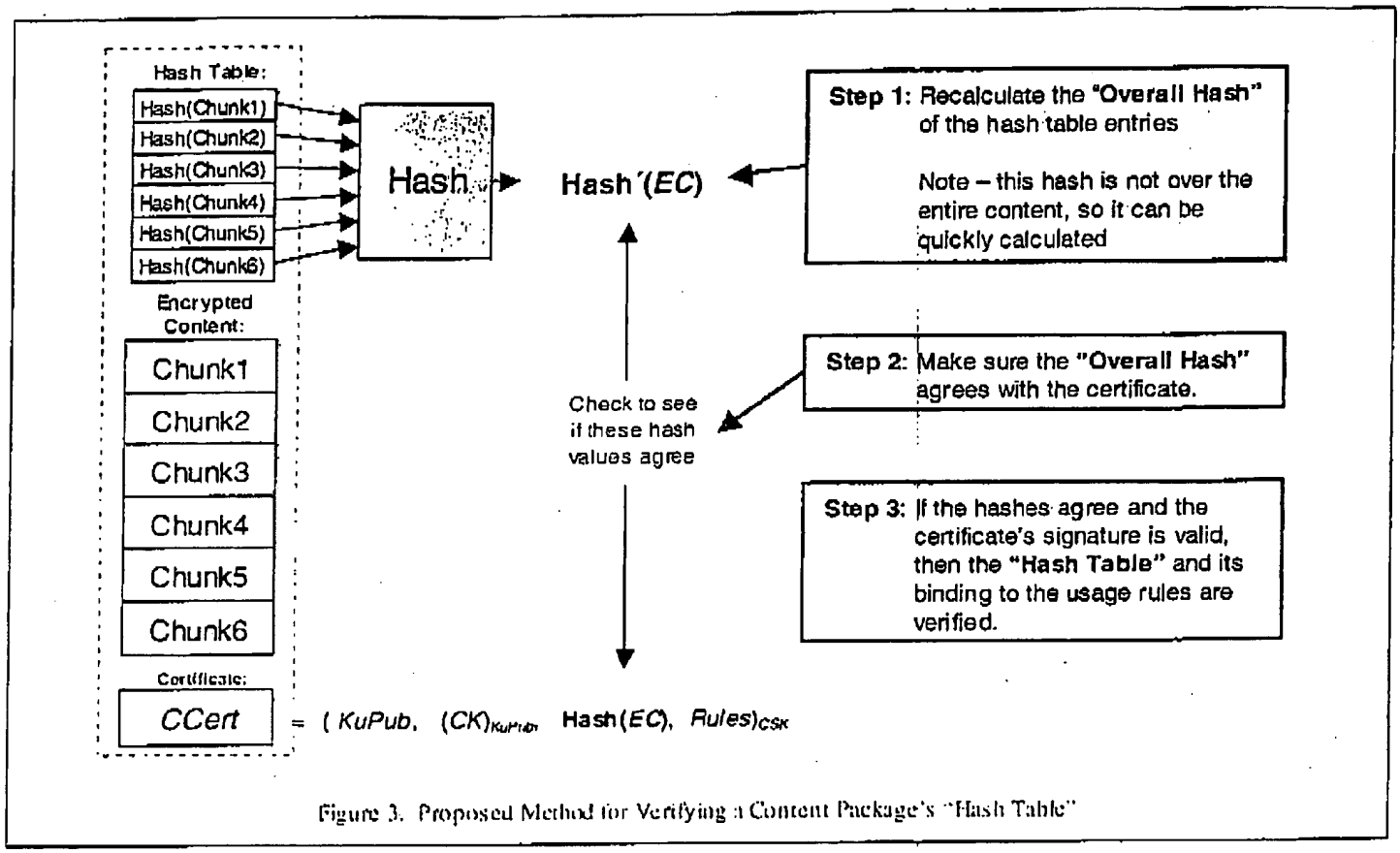

Figure 3. Proposed Method for Verifying a Content Package's "Hash Table"

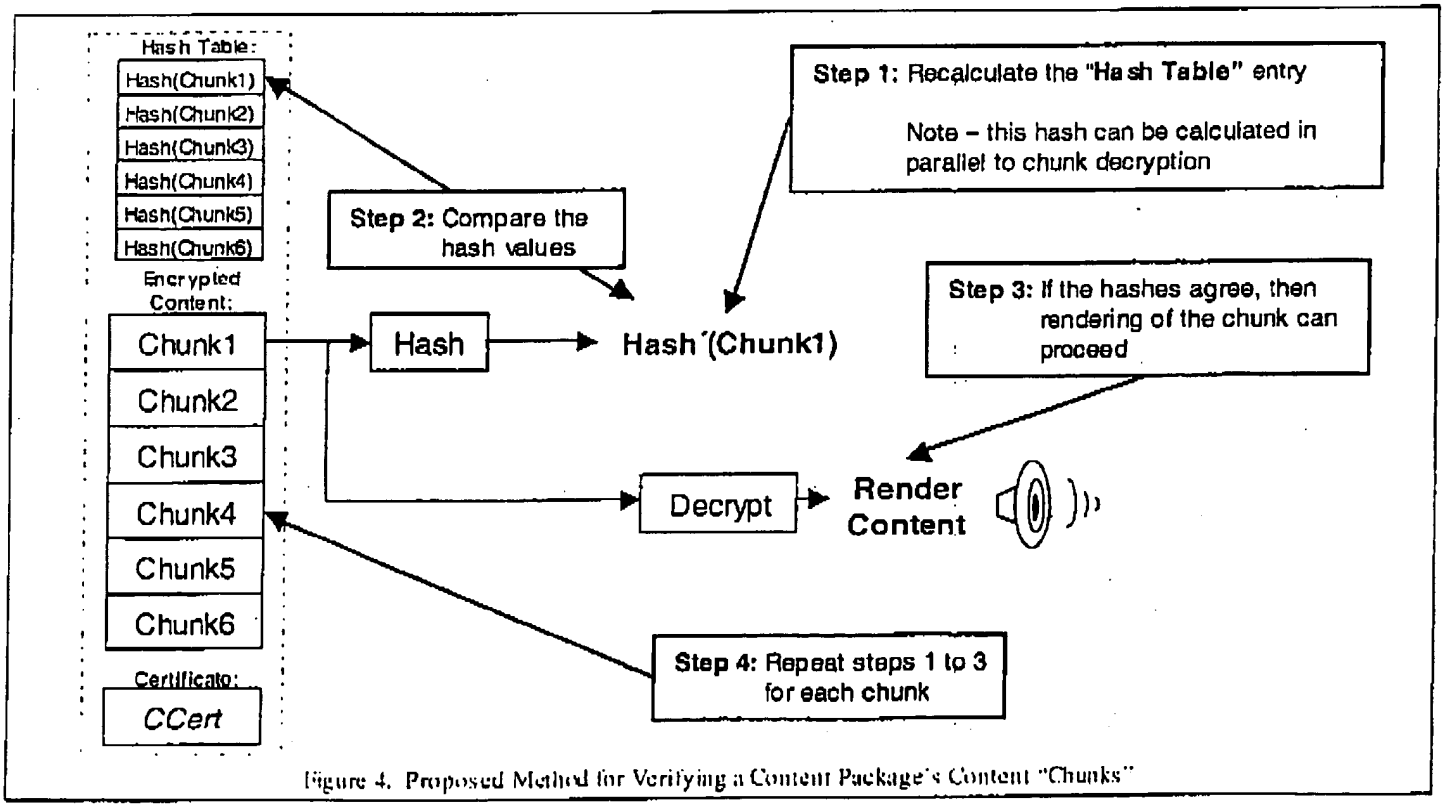

Figure 4. Proposed Method for Verifying a Content Package's Content "Chunks"